I.J. Education and Management Engineering, **2019, 2, 1-14**
Published Online March 2019 in MECS (http://www.mecs-press.net)
DOI: 10.5815/ijeme.2019.02.01

Available online at http://www.mecs-press.net/ijeme

Security Risk Analysis in Online Banking Transactions: Using Diamond Bank as a Case Study

Joseph A. Ojeniyi, Elizabeth O. Edward, Shafii M. Abdulhamid

[a] *Department of Cyber Security Science, Federal University of Technology Minna, Niger State, Nigeria*

Received: 30 October 2018; Accepted: 17 December 2018; Published: 08 March 2019

Abstract

This study is devoted to evaluating the security risk analysis and management in Online Banking transactions using Diamond Bank PLC, Nigeria among other banks. In this paper, a research was carried out in order to evaluate the security risk analysis and management in online banking transactions through the use of the questionnaire to determine the level of risk that customers of financial institutions are likely to encounter. The study indication shows that awareness need to be intensified in terms of risk associated with clients saving password and other transaction details in their devices used in performing an online transaction. Also, the bank should improve on their banking transaction application in order to maintain integrity in view of customer account information.

Index Terms: Risk Management, Online Transactions, Risk analysis, Internet Banking.

1. Introduction

In the world today, there is a proliferation of online access to services. This has also led to online banking where banking services are offered through the internet. Internet banking relates to systems that allow bank customers to access accounts and overall information on bank products and services via a personal computer. Internet banking permits customers to carry on financial transactions in a trustworthy website run by their retail or virtual banks, credit union or building organization. Internet banking products and services can include wholesale products for a corporate customer as well as retail and fiduciary products for consumers [8].

Ultimately, the products and services obtained through Internet banking may mirror products and services

* Corresponding author.
E-mail address: ojeniyija@futminna.edu.ng, lizysteve@yahoo.com, shafii.abdulhamdid@futminna.edu.ng

offered through other bank delivery channels. Some examples of wholesale products and services include cash management, wire transfer, Automated Clearing House (ACH) transactions, Bills presentation, and payment. The example of retail and fiduciary; by products and services include Balance inquiry, Funds transfer, downloading transaction information, Bill presentation and payment, Loan applications, Investment activity, and other value-added services.

Banking sector relies heavily on information system which comprises computers, network, databases, servers, business and customers' information that need to be highly protected from cyber-attacks. No business can be said to be completely secure as there are lots of vulnerabilities in the banking system as well as the information systems used in providing the services. Hence, a need for an information security program that will enable banks to manage the threats associated with internet banking and provides adequate security measures to safeguard important business information as well as the information of their customers and other stakeholders in the financial sector.

The aim of this paper is to perform the security risk analysis and management in online banking transactions using Diamond Bank PLC, Nigeria as a case study. The study is meant to assess the security risk associated with online transaction components in order to ascertain the security priority level required to ensure their confidentiality, integrity, and availability.

2. Related Works

In [8], it was discovered that the implementation of biometric technology plays a major role in controlling the risk factor by using the authentication system. Meanwhile, to achieve an optimal result, planning is of the most important in terms of risk analysis. Furthermore, it was buttressed that assessment of risks should be of foremost interest prior to the implementation of authentication methodology in the internet banking system. For further enhancement on the authentication methodologies, adherence to the security standards is required as may be laid out by the banking information security framework.

[6], evaluate the characteristics of banking risk. They came up with the Bayesian theorem and extreme value theorem which was claimed they are very effective tools in evaluating the assessment of risks in the banking system. Though application of these methods was said to have a challenge of imperfection due to the information systems of banks. To achieve an optimal analysis of data, an integrated system risk management and finance need to be established based on a modern analytical system.

[9], Used k-Nearest Neighbor algorithm in order to establish the most effective feature that aids in a decision-making process, while a feature selection process was achieved using Microsoft SQL server analysis which gave the following results: Reduction of 47 attributes into 17 significant attributes of the features.

[8], In the study, it was revealed that in a banking environment, attaining high levels of business information integrity and overcoming user's security, fears are of most important. More also, it showed that more than coping with a technology change, a risk management plan should manage the issues related to the ethical and social areas. However, the key aspects to a faultless security solution that could meet future needs are well-formulated management strategies, security policies, and data management processes that are built with the necessary flexibility. The study also shows that strategy fit with proper, adaptable and justifiable information security solutions that handles various social, ethical and technological issues would create a friendly and secure environment that would welcome information security banking sectors. They further sought to decide how banks have embraced effective and secure security controls for electronic banking, that incorporate into the banks overall program, including system-wide access controls, user authentication, encryption, Transaction verification, and virus protection controls, and to show how banks have established effective risk monitoring processes, with special stress on security and performance monitoring, as well as audit and quality of assurance reviews.

According to [7], information technology security is of great importance in assessing risk analysis. Hence, it was proposed that qualitative, quantitative and hybrid are methods used in an assessment of security in an information system, also OCTAVE and IRAM are tools employed to perform risk assessment in information

security. however, various assets and vulnerabilities involved in distributed banking applications have been identified using qualitative, quantitative and hybrid methods and tools such as OCTAVE and IRAM have been used.

In [4] the study shows that fears are of utmost concern in conquering users security and to achieve high levels of business information integrity. More also, it was clearly proved that more than coping with a technology change, a risk management strategy should manage the issues related to the ethical and social areas. However, to create a good and secure environment that would embrace information security in banking sectors, a strategy fit with proper, versatile and tenable information security solutions need to be put in place that would address various social, ethical and technological issues. [5] Analyses the relationship of information technology risk factors by examining why information security should be of most important for businesses and also addresses how a security expert can model potential losses for their organization. Furthermore, in the context of internet banking, investigation of information system security was put forward which proves that attention to the importance of security in financial transactions is significant.

In [3] observed the distinctive techniques adopted by the banking industry for risk management such as GAP analysis, value at risk, risk-adjusted rate of return on capital, securitization and internet rating system. However, in achieving this, data was collected from secondary sources such as books, journals, and online publications. More also, various risks faced by banks were identified and the process of risk management was developed and analyzed.

According to [2], risk management gives an efficient avenue for measuring security. Although, the existence of risk management approaches come with major shortcomings such as: the demand for very detailed knowledge about IT security sphere and authentic company environment. However, we can be able to unfold enhanced risk management strategies and make more effective scheduling decisions if dependencies can clearly be identified and analyzed. They put forward a management line of attack to handle risk dependency issues. It is very difficult when initiating a system for evaluating and simulating the major hazards as banking systems are very complex with entities, hazards, and uncertainties

In [1], they pinpoint some of the key security risks, protection strategy, and best practices and future security trends associated with mobile banking through mining relevant blog posts. However, mobile banking gives a lot of advantages to both banks and consumers, as security is a significant barrier to the wide adoption of mobile banking applications. Although there is currently a lack of systematic discussion in the literature about the security risks with mobile banking, with the use of mobile banking applications, it is critical for both banks and consumers to be aware of these risks and there is the need to take steps to mitigate the risks.

It is in the light of the reviewed challenges in financial institutions as it relates to risk analysis and management that envisage security risk analysis in online banking transactions.

3. Research Method

This study was put through to analyze information risk associated with online banking transactions using Diamond bank plc, Nigeria as a case study. The primary source of data was collected using a structured questionnaire which was designed to analyze the threat to information security of financial transactions in the banking sector. The questionnaire was developed using Google Form and was administered to bank users across different geopolitical zones in Nigeria.

The research instrument was self-administered. The respondents were the risk managers in each of the banks. A two-week period was given for the respondents to fill in the questionnaires after which they were collected for analysis. For the analysis of responses, a simple descriptive analysis that comprises of frequency and percentage was performed, while the presentation of results was done using tables and charts.

A scale rating system of very frequently, frequently, occasionally, rarely and never was used in administering the questionnaire in order to obtain responses from the respondents. Furthermore, in order to be able to obtain the risk impact that is associated to online banking transaction, a merging of the scale rating system was carried out in the following format: the merging of very frequently and frequently scales resulted in

the value of low impact risk, while medium risk impact was directly mapped to occasionally scale, the value of high impact risk was obtained through the merging of rarely and never scales.

4. Results and Discussion

A. Demographic Details of Respondents

Table 1., shows the age distribution of respondents. 18% are between the age brackets of 19-30 years, 44% are between the age bracket of 31-40 years while 38% are between the age bracket of 41 years and above, this shows that the respondents between the age bracket of 41 years have been banking with Diamond bank for a very long time.

Table 1. The Age Distribution of Respondents

Age	19-30 years	31-40 years	41 and above
Percentage(%)	18	44	38
Number of respondents	36	22	19

Table 2. Gender Distribution of Respondents

Gender	Male	Female
Percentage(%)	80	20
Number of respondents	40	10

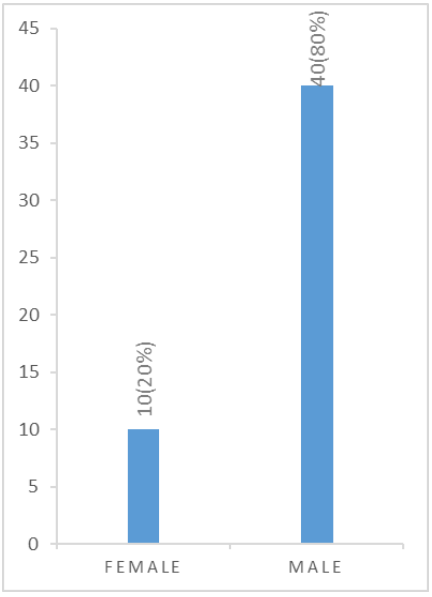

Fig.1. Gender Distribution

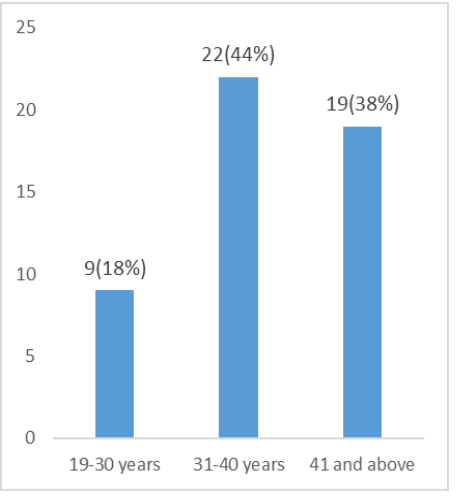

Fig.2. Age Distribution

In table 2., it shows that majority of the respondents who perform banking transactions are males compared to the females from their responses. The study discovered that 80.0% of the respondents are male which amounts to (40) respondents. While 20.0% are female with ten (10) respondents, which indicate that the males are mostly involved in online financial transactions. The respondents that are between the age of 19 – 30years are nine (9) in number, the respondents that are between the age of 31-40 years are twenty-two (22) in number, while the respondents between the age bracket of 41 years and above are nineteen (19), indicating that most of the respondents between the age bracket of 31-40years are mostly involved in online financial transaction activity. The results are shown in fig. 1., and fig. 2., below.

Fig. 3., above shows the years of experience the respondents have been banking. Five (5) of the respondents have 0-5 years of banking experience, sixteen (16) of the respondents have 6-10 years of banking experience. While fifty-eight (58) of the respondents have 1 1years and above of banking experience. This show that most of the respondents have a good number of years of banking experience.

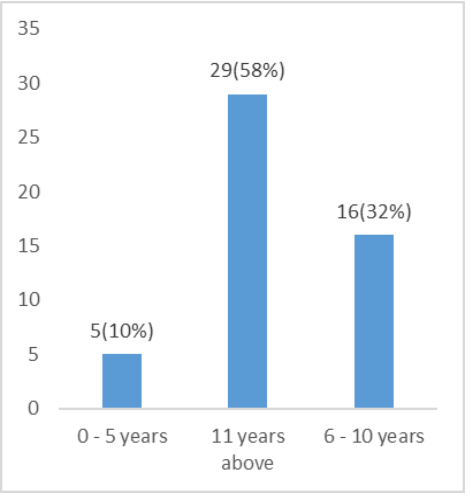

Fig.3. Frequency of Banking.

Fig. 4., shows how often respondents use their device for online financial transactions.2.0% of the respondents indicates that they have never used their device, 8.0% indicates that they rarely use their devices. 2.0% indicates that they occasionally use their devices, 34.0% indicates that they frequently use their devices, while 36.0% of the respondents indicate that they use their devices very frequently for online financial bank transactions. The study shows that the majority of bank users frequently use their device for online financial transactions.

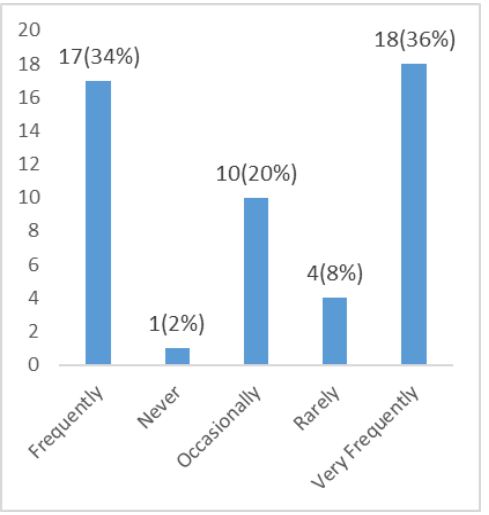

Fig.4. Frequency in using a Smartphone

Fig. 5., shows that 6.0% of respondents are frequently debited without successful completion of online financial transactions, 8.0% are never debited, 8.0% are debited very frequently, 36.0% are rarely debited, while 42.0% of the respondents are occasionally debited without successful completion of online financial bank transactions.

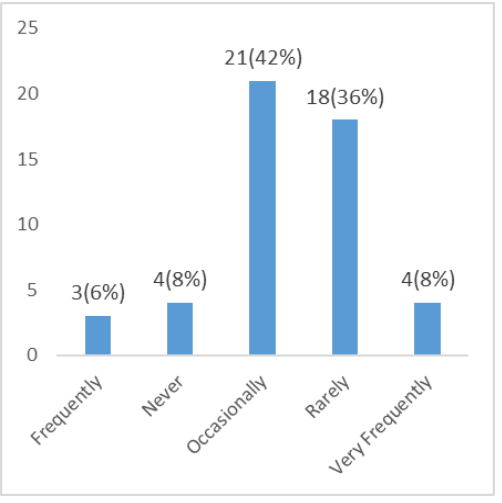

Fig.5. Frequency of being debited without a Successful Transaction

Fig. 6., shows that 4.0% of the respondents are rarely credited for the refund of the unsuccessful online financial transactions, 6.0% are never credited, 12.0% are occasionally credited, 14.0% are credited very frequently, while 64.0% of the respondents indicated that their bank accounts are frequently credited for the refund of unsuccessful online financial bank transactions.

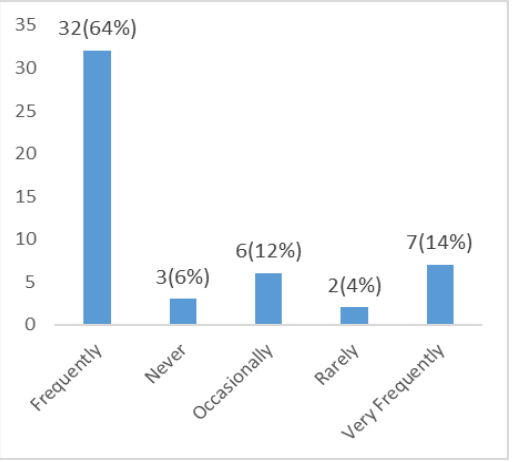

Fig.6. The Frequency of being Credited.

Fig. 7., shows that 2.0% of the respondents frequently give out access of their online financial transaction password to a third party, 6.0% occasionally give out access, 46.0% rarely give out access of their online financial bank transaction password to a third party. And also, 46.0% of the respondents indicated that they never give out access to their online financial bank transactions.

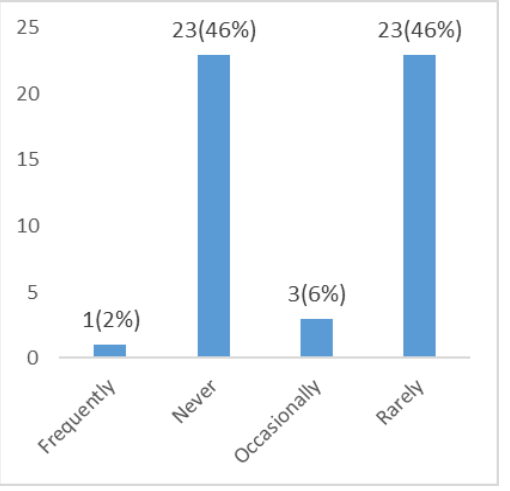

Fig.7. The Frequency of Giving Transaction Access to a Third Party.

Fig. 8., shows that 8.0% of the respondents indicated that their passwords are rarely hacked when performing online financial bank transactions, while 92.0% of the respondents indicated that their passwords have never been hacked whenever they perform online financial bank transactions.

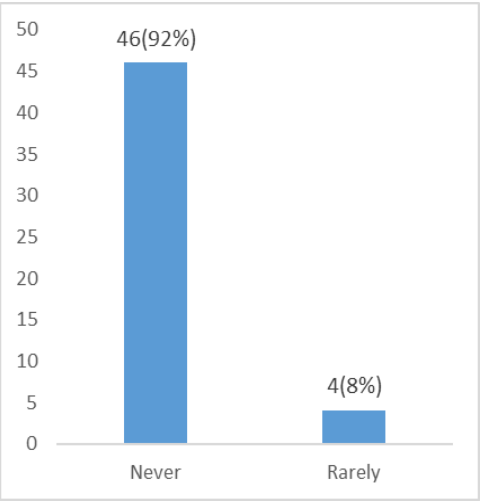

Fig.8. Frequency of Password being hacked.

Fig. 9., shows that 8.0% of the respondents indicated that they have never changed their passwords for online transactions, 38.0% indicated that they rarely change their passwords, 12.0% indicated that they frequently change their passwords, while 42.0% indicated that they occasionally change their passwords for their online transactions.

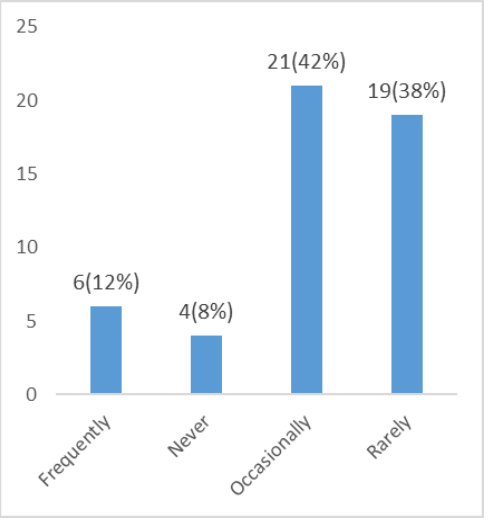

Fig.9. The Frequency of Changing a Password.

Fig. 10., shows that 12.0% 0f the respondents indicated that they frequently save their passwords on their devices, 12.0% also indicated that they save their passwords on their devices very frequently, while 24.0% indicated that they rarely save their online financial passwords on their electronic devices, and 36.0% of the respondents indicated that they have never saved their online transaction passwords on their electronic devices.

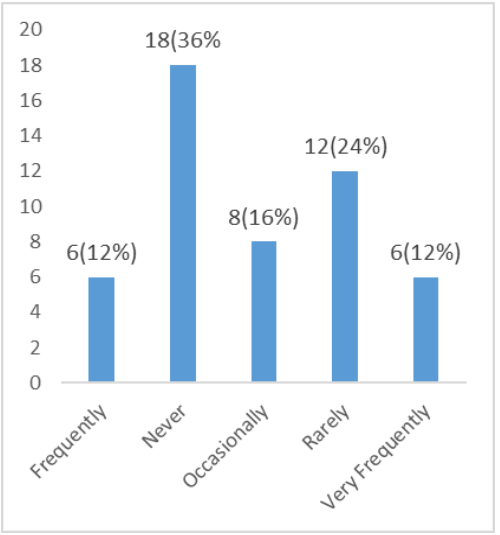

Fig.10. The Frequency of saving Transaction Password on a Device.

Fig. 11., shows that 4.0% of the respondents indicated that they frequently use unsecured wireless access point for online financial bank transactions, also 4.0% indicated that do use unsecured wireless access point very frequently, 30.0% rarely use unsecured wireless access point, while 32.0% of the respondents indicated that they have never used an insecure free wireless access point for their online financial transactions.

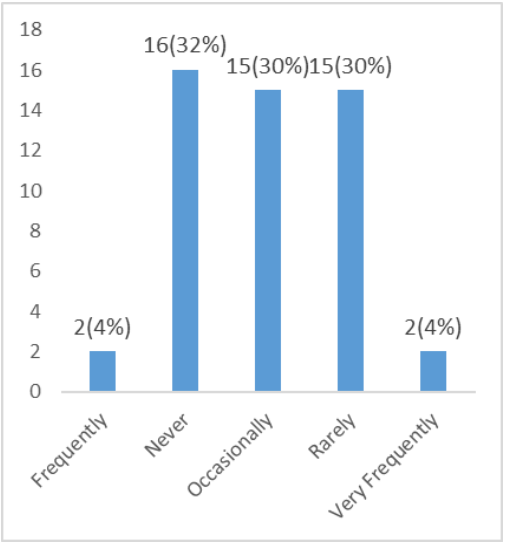

Fig.11. The Frequency of using an Unsecured Free Wireless Access Point.

Fig. 12., shows that 2.0% of the respondents indicated that they rarely use online bank transactions, 4.0% indicated that they have never carried out online bank transactions, 18.0% indicated that they occasionally perform online bank transactions, 40.0% indicated that they frequently use online transactions, while 36.0% of the respondents indicated that they perform online bank transactions very frequently.

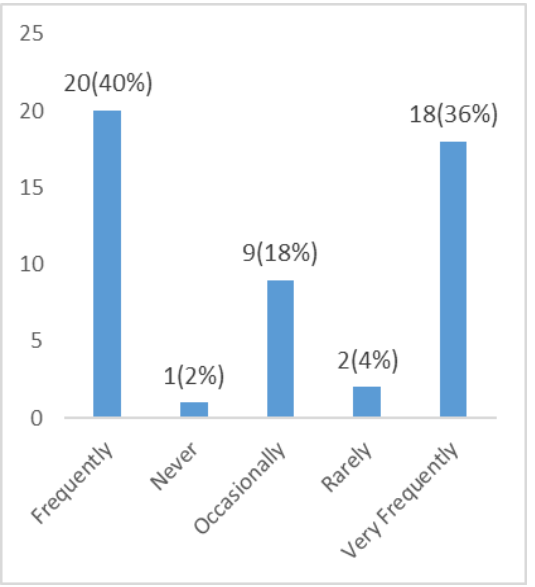

Fig.12. The Frequency of using Online Bank Transaction.

B. The Responses Obtained from Diamond Bank Users

The responses gathered from the respondents showed that six (6) respondents are banking with Diamond bank plc, Nigeria. Diamond Bank Plc ("Diamond Bank") is Nigeria's fastest growing retail bank. Through innovation and technology, Diamond Bank enhances customer experiences and drives financial inclusion in what is called 'Beyond Banking'.

They offer a full range of banking products and services in retail, business and corporate banking segments. Diamond Bank Plc began as a private limited liability company on March 21, 1991 (the company was incorporated on December 20, 1990). Ten years later, in February 2001, it became a universal bank. In January 2005, following a highly successful Private Placement share offer which substantially raised the Bank's equity base, Diamond Bank became a public limited company.

Since the Bank was incorporated in December 1990, Diamond Bank has challenged the market environment by introducing new products, innovative technology and setting new benchmarks through international standards.

Today, Diamond Bank is best placed to respond to changing lifestyles and is leading the digital transformation in response to these societal shifts. For example, Diamond Mobile is Africa's leading banking app and the first with touch ID.

The table 3., below gives a breakdown of the responses obtained basically from those who bank with DIAMOND bank of Nigeria, plc. A five scale rating was used for the questionnaire which is as follows: very frequently, frequently, occasionally, rarely and never. The impact level was also determined. For the low impact we have very frequently and frequently merged, for medium occasionally was mapped, for high rarely and never were merged together. The table 3., below shows a breakdown of impact based on responses obtained about some components in performing online financial bank transactions.

Table 3. Impact of Important Components in Performing Online Financial Bank Transactions

Administered Questions	Scaling Rate	Responses	Percentage (%)	Impact	Overall Impact
How often do you use an online bank transaction?	Very frequently	18	36	Low(38)	Low
	frequently	20	40		
	occasionally	9	18	Medium(9)	
	rarely	2	36	High(3)	
	never	1	2		
How often do you use your device (Smartphone, computer, IPAD etc) for an online financial transaction?	Very frequently	18	36	Low(35)	Low
	frequently	17	34		
	occasionally	10	20	Medium (10)	
	rarely	4	8		
	never	1	2	High(5)	
How often do you save your online financial transaction password on your electronic device?	Very frequently	6	12	Low(12)	High
	frequently	6	12		
	occasionally	8	16	Medium(8)	
	rarely	12	24	High(30)	
	never	18	36		
How often is your bank account debited without successful completion of an online financial transaction?	Very frequently	4	8	Low(7)	High
	frequently	3	6		
	occasionally	21	42	Medium(21)	
	rarely	18	36	High(22)	
	never	4	8		
How is your bank account credited for the refund of the unsuccessful online financial transaction?	Very frequently	7	14	Low(39)	Low
	frequently	32	64		
	occasionally	6	12	Medium(6)	
	rarely	2	4	High(5)	
	never	3	6		
How is your bank account credited for the refund of the unsuccessful online financial transaction?	Very frequently	7	14	Low(39)	Low
	frequently	32	64		
	occasionally	6	12	Medium(6)	
	rarely	2	4	High(5)	
	never	3	6		
How often do you give access to your online financial transaction password to a third party?	Very frequently	0	0	Low(1)	High
	frequently	1	2		
	occasionally	3	6	Medium(3)	
	rarely	23	46	High(46)	
	never	23	46		
How often is your password hacked for an online financial transaction?	Very frequently	0	0	Low(0)	High
	frequently	0	0		
	occasionally	0	0	Medium(0)	
	rarely	4	8	High(50)	
	never	46	92		
How often do you change your online financial password	Very frequently	0	0	Low(6)	High
	frequently	6	12		
	occasionally	21	42	Medium(21)	
	rarely	19	38	High(23)	
	never	4	8		
How often do you save your online financial transaction details on your electronic device	Very frequently	2	4	Low(9)	High
	frequently	7	14		
	occasionally	15	30	Medium(15)	
	rarely	17	34	High(26)	
	never	9	18		
How often do you use unsecured free wireless access point (e.g hotspot) for an online financial transaction	Very frequently	2	4	Low(4)	High
	frequently	2	4		
	occasionally	15	30	Medium(15)	
	rarely	15	30	High(31)	
	never	16	30		

Based on the information gathered from the responses in the table above, it was discovered that most of the respondents save their online transaction passwords and their transaction details on their devices. This can serve as a potential risk to the respondents if a third party has access to the electronic device used for the online transactions. Therefore, Diamond bank need to sensitize their clients on how to manage their passwords and their online details when performing online financial transactions. Also, customers are often debited without a successful online transaction and they are not frequently credited. As a result, the diamond bank needs to improve on their transaction web applications. The bank needs to enlighten her clients on the risk of giving out their online financial transaction passwords to a third party because the potential risk is high. In using a free wireless access point, your transactions can still be hijacked by a malicious entity. In order to stop this, Diamond bank need to create awareness for their customers using a free wireless access point.

In table 4., it is shown that respondents have good background knowledge in banking transactions. Twenty-nine (29) of the respondents have 11 years and above of banking experience, sixteen (16) have 6-10 years of banking experience, while five (5) 0f the respondents have 0-5 years of banking experience.

Table 4. Respondents Experience with Online Transaction

Years of banking experience	0 – 5 years	6 – 10 years	11 years and above
Percentage (%)	10	32	58
Number of respondents	5	16	29

5. Conclusion and Recommendation

The study discovered that most of the respondents have fundamental knowledge of security risk in terms of disclosing their online bank transactions details, indication shows that more need to be done in terms of bank client awareness about saving transaction details and passwords on transaction devices. Also, the bank should improve on the banking transaction applications in order to maintain banks integrity in view of customer account information.

References

[1] W. He, X. Tian, and J. Shen, “Examining Security Risks of Mobile Banking Applications through Blog Mining,” 2014.

[2] K. Subrahmanyam, M. Haritha, V. Tejaswini, C. Balaram, and C. Dheeraj, "Information Security and Risk Management for Banking System Nomenclature : Major Aspects : Information Security ," vol. 10, no. 3, pp. 171–176, 2014.

[3] T. Kanchu and M. M. Kumar, “RISK MANAGEMENT IN BANKING SECTOR -AN EMPIRICAL STUDY,” vol. 2, no. 2, pp. 145–153, 2013.

[4] C. Odhiambo, N. Joe, and E. Abade, "Evaluation of Information Security Risk Assessment for Internet Banking Among Commercial Banks in Kenya," vol. 5, no. 3, pp. 51–59, 2016.

[5] V. R. Ambhire and P. S. Teltumde, “Information Security in Banking and Financial Industry,” vol. 14, no. October, pp. 101–105, 2011.

[6] Chornous, G., & Ursulenko, G. (2013). Risk Management in Banks: New Approaches to Risk Assessment and Information Support. Ekonomika, 92(1), 120–132.

[7] Kiran, K. V. D., Sruthi, P., Neema, P. S., Vani, G. V. S. M., & Sahu, R. (2014). Risk Assessment in Online Banking System, 9(6), 279–285.

[8] Sarma, G., & Singh, P. K. (2010). Internet Banking : Risk Analysis and Applicability of Biometric Technology for Authentication. International Journal of Pure and Applied Sciences and Technology, 1(2), 67–78.

[9] K. Elissa, "Title of paper if known," unpublished. Sobhy, M., Abbas, S., & Salem, A.-B. M. (2015). Knowledge Discovery for Banking Risk Management. Proceedings of the International Conference on Intelligent Information Processing, Security and Advanced Communication - IPAC '15, 1–6. https://doi.org/10.1145/2816839.2816853.

Authors' Profiles

Joseph A. Ojeniyi, is a lecturer in the Department of Cyber Security Science, School of Information and Communication Technology, Federal University of Technology (FUT) Minna, Nigeria. He received his Ph.D. in Cyber Security Science from the same University, M.Sc. in Computer Science from the University of Ibadan, Nigeria, and a B.Tech. in Mathematics/Computer Science from FUT Minna, Nigeria. He has been appointed as a reviewer to several indexed Journals. He currently serves as the chairman of the Conference Organizing Committee of the faculty, 'ICTA 2018'. His area of interest includes Cyber Security, Digital Forensics, Deep Learning, Artificial Intelligence in Information Assurance/Security and Cyber-Physical Systems.

Shafi'i Muhammad ABDULHAMID received his Ph.D. in Computer Science from University of Technology Malaysia (UTM), MSc in Computer Science from Bayero University Kano (BUK), Nigeria and a Bachelor of Technology in Mathematics/Computer Science from the Federal University of Technology Minna, Nigeria. His current research interests are in Cyber Security, Cloud Computing, Soft Computing, Internet of Things Security, Malware Detection and Big Data. He has published many academic papers in reputable International journals, conference proceedings, and book chapters. He has been appointed as an Editorial board member for the Journal of Computer Science and Information Technology (JCS). He has also been appointed as a reviewer of several ISI and Scopus indexed International journals such as Journal of Network and Computer Applications (JNCA) Elsevier, Applied Soft Computing (ASOC) Elsevier, Journal of King Saud University Computer and Information Sciences (JKSU-CIS) Elsevier, Neural Computing and Applications (NCAA) Springer, Cluster Computing Springer, Egyptian Informatics Journal (EIJ) Elsevier, IEEE Access Journal (U.S.A.), Wireless Networks Springer, Plos One Journal, an International Journal Engineering Science and Technology (JESTHC) Elsevier, Brazilian Journal of Science and Technology (BJST) Springer to mention but a few. He has also served as Program Committee (PC) member of many National and International Conferences. He is a member of IEEE Computer Society, International Association of Computer Science and Information Technology (IACSIT), Computer Professionals Registration Council of Nigeria (CPN), International Association of Engineers (IAENG), The Internet Society (ISOC), Cyber Security Experts Association of Nigeria (CSEAN) and Nigerian Computer Society (NCS). Presently he is a Senior Lecturer in the Department of Cyber Security Science, Federal University of Technology Minna, Nigeria and is currently supervising both Masters and Ph.D. students (in both Nigeria and Malaysia). research fields include cloud computing computer science cybersecurity information and computing sciences soft computing software engineering.

Elizabeth. O. Edward is a master student in the department of cybersecurity science, school of information communication technology, federal university of technology (FUT) Minna, Nigeria she received her BTech in computer science from Ibrahim Badamasi Babangida University Lapai, Nigeria. Her area of interest includes computer networking security, information security Risk and management.

How to cite this paper: Joseph A. Ojeniyi, Elizabeth O. Edward, Shafii M. Abdulhamid,"Security Risk Analysis in Online Banking Transactions: Using Diamond Bank as a Case Study", International Journal of Education and Management Engineering(IJEME), Vol.9, No.2, pp.1-14, 2019.DOI: 10.5815/ijeme.2019.02.01